Insurgencies in the Infosphere

Air Command and Staff College – Small Wars Research Elective

Lieutenant-Colonel William Dupuy
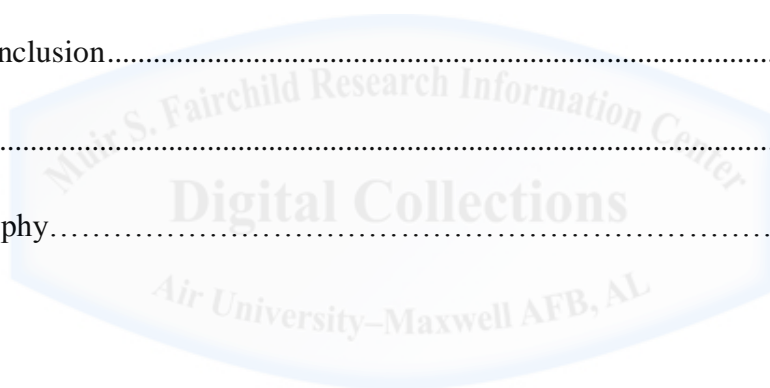French Air Force

DISCLAIMER

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

1. Table of Contents

1. Introduction

Militaries have in most cases considered insurgencies as a perverted and improper form of war. Napoleon the 1st, so brilliant at fighting big, decisive battle, was never quite able to understand the insurrection that followed his successful invasion of Spain. The US military won the conventional war in Iraq in months, but failed to end the ensuing insurrection in years. Even today, after two major insurrections fought in parallel, the major military powers still design their weapons, tactics and training for the next conventional war, considering that high intensity tools will do well for low intensity conflicts. Yet, counterinsurgency has focused most of Western military efforts in the past decade. In Afghanistan like in Iraq, after quick conventional victories, most soldiers have wondered how to terminate a conflict against foes that fragment when attacked and regenerate faster than they can be rendered ineffective.

To deal with the timeless phenomenon of insurrections, two major competing theories have been proposed. On the one hand, the enemy-centric approach aims at destroying enemy assets, leadership and forces faster than they can rebuild. On the other hand, the population-centric approach focuses the civil-military effort on gaining the "hearts and minds" of the population, assuming that without popular support, an insurgency is unable to develop and fades rapidly.

Both approaches have earned successes and endured setbacks. And the best solution seems so far a balance of both approaches. Therefore no unifying theory allows a comprehensive understanding of insurgency and counterinsurgency strategies. I will argue that due to the political nature of insurgencies and the evolution of the Information technologies, an analysis of modern insurgencies as a struggle to prevail in local and global Infospheres best

explains these phenomena. Therefore, an Information-centric strategy is probably the best approach to understand and fight modern insurrections.

To understand the tenets of this approach, it is first necessary to acknowledge that classical theories of insurgencies fail to fully grasp the stakes of this form of conflict, and cannot explain modern, transnational insurrectional phenomena. Therefore, I will describe succinctly the classic approach to insurgencies, and then explain why each provides only an incomplete view of the phenomenon.

Next, I will define the Infosphere and describe its tenets and its most significant characteristics for this study. I will also explain how insurgents and counterinsurgents fight in this new environment.

Finally, I will show that an analysis of the impacts and actions in the Infosphere provides a better understanding of insurrectional phenomena, whether they are of national, transnational or international nature.

2. Classical approaches to insurgencies

Classical strategists did not actually study insurgencies as a specific phenomenon. For example, Clausewitz wrote "We may occupy a country completely, but hostilities can be renewed again in the interior, or perhaps with allied help. (…)We must always consider that with the conclusion of peace the purpose of the war is terminated."[1] Nevertheless, major thinkers of insurgencies later developed several approaches to understand insurgencies and define effective strategies. We can divide them into three main trends: enemy-centric, population-centric approach, and leadership-centric.

2.1. Enemy-centric approach

Described for instance by Calwell in his Counterinsurgency Manual[2], this approach was followed by colonial empires until the end of the XIXth century, and occasionally by powers fighting a consistent and identifiable armed opponent. The purpose of this approach is clearly to eradicate the insurgency forces, just as an army is trained to subdue a foe. In many cases, modern armies still tend to privilege this approach for two reasons. First, their training teaches them to fight this kind of conflict. Moreover, many modern insurgencies have begun with a conventional war and turned to guerrilla warfare when the balance of power shifted. Operation Iraqi Freedom, for instance, began as a regular war, and turned to guerrilla warfare after the fall of Saddam Hussein's regime. This approach is still employed, at least besides the others. In Afghanistan, the killing of Taliban and Al Qaeda leaders aims at disorganizing the insurgency and weakening it by depriving it of its key elements. The underlying idea is then to force the insurgency to adapt faster than it is actually able to. By neutralizing key elements (leaders, funders, etc.), the insurgency is expected to lose key skills and abilities hard to replace.

2.2.Population-centric approach

In the late nineteenth century, some military leaders realized that the enemy-centric approach failed to embrace the political aspect of this kind of conflict. "Revolutionary war is a political war"[3], Galula wrote. Indeed, he said, "the battle for the population is a major characteristic of the revolutionary war."[4] This approach, earlier developed by Gallieni under the name of "tâche d'huile", makes of the local populations the center of gravity of the conflict. Acknowledging that part of them provides the insurgency with fighters, asylums from counter-insurgents and support, this approach aims then at winning the "hearts and minds". The whole strategy is then to provide security to a limited population, gain its support and isolate it from insurgents' influence, and then expand this approach to another area.

2.3.Other tentative approaches: Leadership-centric

Lately, several approaches focused on leadership and organizations. Moyar emphasized the importance of an adaptive and effective leadership. He wrote, "Counterinsurgency is leader-centric warfare, a contest between elites in which the elite with superiority in certain leadership attributes usually wins."[5] Nagl studied the ability of an organization to take rapidly into account the lessons learned, and linked this learning ability to effectiveness in insurgencies. For both, the ability of organizations (for Nagl) and individual leaders (for Moyar) to be flexible enough to adapt to the conflict is the key to success.

3. Limitations of the classical approaches

Although each of these approaches turned out to be useful, they do not offer a unified understanding of the situation. For example, in Afghanistan, the US military follows at the same time a population centric approach through Provincial Reconstruction Teams, and enemy centric

operations inspired by the leadership centric concept that emphasize the elimination of key leaders of the insurrection. Each of these approaches has critical limitations.

3.1.Enemy-centric limitations

The enemy-centric approach showed its limitations when the insurgents had consistent popular support and little military assets. Under such conditions, armies can hardly fight their opponent because the latter avoids confrontation, and provokes military violence to gain more partisans. Moreover, killing or disrupting the enemy no longer brings a strategic advantage, given that the population will provide new combatants. Finally, thanks to modern communication technologies, the insurgencies can apparently disperse and spread their forces while keeping their destructive power.

3.2.Population-centric issues

Likewise, population-centric approaches have been fruitful when the communication lines and the populations' cultures allowed the counter-insurgents to filter into a given area, and deny effectively the insurgency any influence inside it. However, several variables can make this strategy less effective. Indeed, the extent of physical and electronic communications has dramatically increased. It becomes then harder and harder to have an extensive informational control over an area. Whatever the isolation of an area, mass media, cellular phone and Internet offer insurgencies the ability to broadcast their ideologies, achievements and points of view. Besides, this approach involves the reestablishment of economic activity in the safer areas. Consequently, the traffic of people and goods in and out of the area increases. And so, the more successful the population-centric approach is to reestablish a "normal life" in a given area, the more vulnerable this area becomes from insurgents intrusions and influence. Finally, global insurgencies like the spread of communist cells in the 70s or the actual Islamist insurgency led

by Al Qaeda, do not allow for this kind of method. Population centric approach is local in nature; it is then essentially insufficient against a global enemy. Another paradigm is therefore necessary to deal with this new phenomenon.

3.3. Leadership centric: an actual approach?

The leadership-centric approaches are valid in that they furnish ways for leaders and organizations to enhance the effectiveness of their actions. Nevertheless, they are of little help in analyzing an insurgency and defining a strategy. They do not try to explain the phenomenon or to provide the leader with a way to understand his or her adversaries. They are self-centered, focused on one's own forces and weaknesses, and so cannot help us to understand and react to an insurgent's strategy. Moreover, as Moyar pointed out, finding enough leaders having these qualities, experience and flexibility is not that easy. Thus, although Templar in Malaya could select civil and military leaders from the whole British empire to fight his insurgency, he also had to reduce the size of police forces because he lacked enough good leaders in this area.

3.4. Unaddressed Issues

An insurgency is probably one of the most complex phenomena to analyze. It usually takes root in popular discontent (economy, political system), but needs a set of favorable factors to develop and succeed. Among those, the "cause" (as defined by Galula) plays several roles. It conditions the popularity and legitimacy of the movement, and may foster international support. Therefore, any study of an insurrection disregarding some factors as cultural basis, strength and support of the cause, external supports and international legitimacy necessarily fails to grasp some essential tenets of the phenomenon.

3.5.Modern insurgencies

According to Hammes, the insurgencies fought after WW2 are an indication of a fundamental shift in the art of war, driven by a new paradigm, which he calls 4G Warfare. Thus, modern insurgencies have emerged as an adaptation to three main factors.

First, the Cold war saw the Great Powers acquire arsenals of tremendous power and overwhelming superiority. Therefore, it was no longer relevant for any regional power threatened by those superpowers to engage a conventional fight. Whatever the relevance of the strategy, the war was lost if waged frontally. For such challengers (state or non-state actors), it was then necessary to define another paradigm in order to rebalance the chances of success.

Second, globalization is a clear and decisive trend today. Many non-state actors hold power in the areas of economy and finances, information, and ensure critical services to the states. At the political level, international organizations hold a great deal of soft power, so states are no longer fully sovereign when waging war or dealing with insurgencies even within their area of responsibility. This general shrinking of states sovereignty empowers non-state actors (legal, like multinational companies, or illegal like themafia, drug cartels) to challenge locally the power and legitimacy of states.

Third, the evolution of information and communication technologies (ICT) has accelerated tremendously since the 20th century. This evolution has empowered the insurgents, providing them with affordable and effective assets that were once dedicated to states.

Indeed, while long-range communication was expensive and available only to wealthy organizations, satellite communications, wireless phone and communications are now widespread in all parts of the globe and affordable to very small organizations. Consequently,

modern societies gradually become *informational*. This can be understood on two levels. At the

technical level, modern societies are increasingly dependent on IT[1] systems. Most critical

systems like power supply, water, or transportation systems rely on IT networks. The part of the

economy that depends on the internet is growing, while banks and trade systems would be

paralyzed by a failure of their IT systems. On the cognitive level, modern societies are also

immersed in a global infosphere. The convergence of public media and the Internet has made

information available almost instantly, feeding the people around the world through a variety of

channels: radio, television, newspapers, but also various "independent" websites (I mean those

not owned by a traditional media group), Twitter, are only example of channels through which

Information can diffuse. Besides, all these media reproduce themselves in a maelstrom of

information making it sometimes arduous to identify the people absorbing it, the course followed

and the accuracy and origin of said information. The forging of *public opinions* is therefore

increasingly hard to grasp and more critical than ever.

Yet, as Merom emphasized, democratic states have lost recent small wars, not on the

battlefield but precisely through their own public opinion. He wrote, "The primary goal and best

hope for insurgent movements have always been that they will manage to dissuade their

powerful rivals from continuing to fight by imposing on the latter a high enough cost for a long

enough period."[6] It is therefore very inexact to consider an insurgency without taking the

homeland of the counterinsurgent into account. For instance, the impact of terrorist attacks on the

homeland of the counterinsurgent remains a major issue, and it is a part of the same

phenomenon. Thus, Al Qaeda terrorist attacks on a train in Madrid caused Spain to withdraw

---

[1] Information Technology

from Iraq and it was a great achievement for this group. Jenkin explained that the psychological impact of terrorism was above all an outcome of the *perceived* risk of possible future actions, more than a real risk based on precedent terrorist attacks[7]. Given that such issues of perceptions may cause mighty military powers to lose small wars, no relevant analysis should disconnect them from the local problems to solve.

Finally, although global or transnational threats such as Al Qaeda or the Muslim Brotherhood become increasingly significant, none of the former approaches explain them. Yet, analyzing the "War on Terrorism", Kilkullen successfully showed that these movements were best explained as insurrectional phenomena (which allowed an analysis of the aims for instance) than as pointless brutal violence.[8]

For all these reasons, it is therefore necessary to look for a global approach acknowledging the political nature of war, embracing the whole insurgency phenomenon and all its actors, on the battlefield, on public opinion and on the international stage.

4. Insurrections in the infosphere(s)

To grasp the influence of Information in insurgencies, it is first necessary to define the extent of an Infosphere, some key characteristics of this virtual environment and what the struggles within this ecosystem look like.

4.1. Nature of the infosphere

In order to grasp the way information is generated, flows and is acquired, the word *Infosphere* has been subject of several tentative definitions. For Lonsdale, "the infosphere is best thought of as an amorphous entity where information exists and flows."[9] This definition is

interesting, because it is easy enough to grasp and delimit: Infosphere thus encompasses all the technical systems processing and transmitting information. Nevertheless, it remains foggy due to the very nature of information. Indeed, this definition does not explain whether one single global infosphere will be given priority, or if any set of informational entities can be considered as an infosphere. For instance, any contact between two infospheres would obviously induce exchanges of information (at least non-verbal information: the way people behave, dress, etc.).

Therefore, Floridi defined an infosphere in comparison to a *biosphere,* as a whole informational ecosystem, made of media of communication, technical systems but also including the different human actors generating, modifying and absorbing information[10]. This definition is much more interesting for our study because it specifically addresses both the channels of communication and the people issuing and receiving the Information. Thus it is possible to analyze specific issues related to perceptions, such as cultural gaps, misinterpretations for instance. Moreover, it also permits the analysis of several interacting infospheres, each remaining a self-sufficient ecosystem.

To illustrate the notion of infosphere, let us consider a typical, remote village in Afghanistan, at stake for both a Taliban group and the troops of the coalition (ISAF). Under such conditions, we can consider that the Taliban is one infosphere, the village another, the ISAF is a third one, while the international community might be another one. For sure, each interacts frequently with the others. Besides, some villagers may be part of both the village's infosphere and the insurgent group's infosphere. Nevertheless, until the insurgents are part of the village, they will not be part of its infosphere, for they will be considered outsiders and will not be fed by the information. Therefore, coalition and insurgents alike will try to establish trust relationships with the village's infosphere. They will compete to enhance their interactions with the population

13

while preventing the enemy from doing the same. But they will nevertheless mostly remain outsiders.

Information describes any piece of knowledge exchanged in the Infosphere. It can be *explicit*, such as messages exchanged between a command and control system (C2) and combatants, or messages crafted by IO cells and broadcast to populations. But it can also be *implicit* and transmitted through behaviors and actions. Thus, providing security to neutral populations, the counterinsurgent communicates his willingness to address the issues of the populations and its ability to win the conflict.

Communication encompasses all possible ways to deliver a message from the emitter to the receiver. It includes obviously written media, television, radio broadcasts, Internet, but also visible actions from the emitter. Thus, the action of armed forces, police, administration, delivers messages to the population. Likewise, the insurgency, threatening the population through violent actions also delivers messages to the population and to its opponent.

A hard issue in addressing the issues of information during a conflict is its relative universality. Indeed, local events can propagate instantly at the international level. Thus, the famous picture of South Vietnamese General Nguyen Ngoc Loan summarily executing a Viet Cong fighter had tremendous impact on the American public opinion.

Nevertheless, this does not mean that information is homogeneous or instantaneous throughout an Infosphere. First, in some cases, the propagation of information can be slowed down or twisted. Military leaders can choose to "tell their story", that is to say embed journalists in their maneuvers and release material from their operations. Due to their unique position, the military have access to privileged material that is eagerly desirable to the media. Thus, Hoskins

wrote, during Operation Desert Storm, the US military embedded reporter teams in combat operations[11]. This smart choice caused the embedded journalists to live the threats and conditions of the US soldiers and therefore influence their reports. The acknowledged consequence was a strongly biased report of this operation, in favor of the US operation.

Moreover, it is possible to hamper undesired communication. Thus, although Bin Laden's communication through Al Jazeera channels really bothered the coalition in Afghanistan, Taliban communication was relatively scarce due to the cyber- and EW[2] threats they faced. Indeed, they feared to be located and destroyed if they used mobile phones intensively, some of their websites were shut down or infiltrated. So Taliban and Al Qaeda leaders had to rely only on human networks exclusively for the exfiltration of their messages.

4.2. How armed actors embraced this new paradigm

This profound evolution was integrated by regular armies and insurgents in very different ways. While the armed forces emphasized the means of communication as a force multiplier, the insurgent used them as an affordable recruitment medium, an operational asset and an effective way to question the counterinsurgent's legitimacy on the battlefield and in the homeland.

The military and the information

How Western Powers embraced the Information Revolution

To a great extent, the regular military forces embraced the technological improvements in the area of telecommunications to enhance their combat effectiveness through command and control (C2), and intelligence collection and dissemination. As a consequence, what Rid and

---

[2] Electronic Warfare

Hecker named internal communication greatly enhanced the lethality and effectiveness of military regular forces.

Conversely, the external communication, that is to say the messages sent to the national and foreign publics, was initially carefully avoided[12]. The authors noted that *"Military decision makers saw the improved flow of public information as a set of huge problems (…). Commanders regarded the press as a nuisance, not as an integral part of military operations[13]"*. Eventually, given that *"The military is forced to engage the adversary in the informational and cognitive dimensions of Cyberspace"[14],* western countries divided Information activities between Public Affairs and Information Operations, in concordance with the separation of responsibilities between civil and militaries. Indeed, these nations make a clear separation between the political (directed towards populations and governments) and the military (focused against the adversaries)[15]. As a consequence, most modern countries show dramatic deficiencies in their global communication strategy.

Yet, the message conveyed by tactical-level troops usually has strategic level implication. Thus, during the Iraqi counter-insurrection campaign, while the US army aimed at calming down the strains between Sunni and Shia communities to restore a lawful state, "a reporter for *Times Magazine* showed Chiarelli a disturbing video (…). Twenty-four Iraqi had been killed, including some women and children after a bomb attack on a Marine convoy. The Marines hadn't investigated the incident."[16] Such an event, due to a tactical level misunderstanding of the strategic priorities, can jeopardize former efforts of pacification.

Information Operations

The AFDD3-13 stipules, "This integration of influence, network warfare, and electronic warfare operations to create effects on OODA loops is the unifying theme of IO."[17] In the specific case of insurgencies though, most OODA loops of the insurgent assets and goals lie in the Informational area.

Most western military doctrines have regrouped under the unifying term of information Operations, all defensive activities protecting sensitive military information, and offensive ones disrupting the enemy's communication channels or susceptible of modifying enemy and neutral perceptions. These activities can be divided into three categories.

The activities of a *technical* nature are aiming at the *communication* channels. They encompass electronic warfare, computer network operations and operations security.

The activities *dedicated to information* "address the minds (knowledge or emotions)."[18] They encompass operational communication. This mode of action is directed towards one's own troops to reinforce cohesion and legitimacy of the fight, as well as to counter enemy's IOs, but also toward partners and neutral populations at the local, national and international levels. They also include Psychological operations, which aim at convincing the operational environment of the legitimacy and effectiveness of friendly actions.

Finally, the Intelligence activities collect information from diverse origins in order to prepare the action, assess enemy forces and strategy, and reassess friendly strategy.

Informational Insurgents

While this revolution in Information technologies and media created new problems for regular forces, the phenomenon had several positive outcomes for insurgents. It offered a low cost communication infrastructure, allowed affordable C2 systems and gave wide access to local

and worldwide audience. Moreover, the opportunities of communication offered them new horizons. Their political and military branches being usually tightly interconnected (when distinct), their communication strategy is far more coherent and effective.

Indeed, significant asymmetries favor insurgents in the media sphere. "At the heights of unrests in Iraq, the insurgency published more press releases than the American forces in the Middle East"[19] While the regular forces have more power but also more accountability, insurgents have many advantages. For example, they don't have to stick to the truth. Moreover, the show of violence is usually favoring their cause by undermining the perceived ability of power to ensure security.

Finally, the internet granted insurgents such as Al Qaeda an unprecedented audience for recruitment, training and coordination. Similar to the economic "Long Tail" (described as *"the demographics of buyers that purchase the hard-to-find and previously hard-to-sell items"[20]*) concept, the Internet allowed terrorist organizations to reach and recruit very marginal widespread populations around the world.

Defining this new paradigm with the idiom *War 2.0* as a reference to the recent implement of Internet standards (Web 2.0), Rid and Hecker emphasized the shift of the decisive battle into the informational area[21].

5. Towards an Information-centric approach

More than a minor change of the operational environment, the informational arena increasingly decides of the outcomes of the struggle. It is therefore necessary to craft strategies focused on it.

5.1. How classical approaches do in the information area

Each of the former approaches has informational impacts. The enemy centric approach fundamentally aims at deterring the enemy and reducing the opportunities for insurgents to recruit. Indeed, if the attrition rate is important enough among the insurgency, its forces (in the Clausewitzian sense) will decrease: the capabilities of armed forces will be destroyed, and the will to fight may decrease among sympathizers and insurgents. The main goal of enemy-centric approaches is therefore deterrence. Moreover, this approach also shows the will of the counter-insurgent to fight an insurrection and protect institutions and people. Thus, a selective and controlled enemy-centric approach can convey positive messages while hampering enemy informational capabilities.

Likewise, the population centric approach broadly focuses on communication. According to Galula, "facts speak louder than words."[22] Thus, he promoted a limited use of force interdicting insurgents from local areas, then to strict defensive purposes. "The real purpose of the operation, then, is to prepare the stage for the further development of the counterinsurgent action."[23] Therefore, a counterinsurgency campaign aims at convincing the people that the state is a capable actor, able to address the population's grievances and that its eventual prevalence is realistic.

Finally, the leadership centric approach enhances the communication effectiveness of the counterinsurgent. Nagl advocates the learning abilities of an organization, which are particularly important in the area of communication. He wrote, "In a battle against insurgents, persuading fighters to surrender and provide information on their comrades is much more effective than killing them; persuading the masses of the people that the government is capable of providing essential services – and of defeating the insurgents – is just as important."[24] Likewise, Moyar's

19

leadership centric approach allows a more effective low level communication. Indeed, reconciling kinetic operations with effective non-verbal communication is especially hard. Sharlet gave an example of uncontrolled behaviors that conveyed a message obviously opposite to the national intent[25]. During OIF, he says, soldiers forced a translator to write, "Jesus killed Mohammed" on a US tank. Besides the long-term impact of such misconduct, the unit was targeted by insurgents' heavy fire. As a consequence, uncontrolled tactical-level communication, due to inadapted leadership, can lead to major strategic issues.

5.2. Why information is *the* central stake in insurgencies

In his masterpiece "On War", Karl Von Clausewitz wrote that the ability of a nation to fight lay in three major aspects. "The first of these three aspects are the people; the second the commander and his army; the third the government."[26] One of the main issues in insurgencies is precisely to deal with the absence of such coherent, visible trinity. Yet, behind the façade of apparent dispersion, an insurgency pursues a political goal, through violent actions relying on popular support and the armed forces. Only, this trinity is not made of independent elements. These three components are tightly interrelated. Indeed, if one considers an insurgency as a "nation within the nation", the intensity of the popular support provides the insurgency with an "army", that is to say a capacity for action, and legitimacy to the leader. Understanding this central role of the people in an insurrection, Galula, explained the tenets of a population-centric approach.

As he stated, the 'cause' in insurgency has therefore a paramount instrumental role. It is not only the political object of the insurgency, but also the ideological arguments making this political objective relevant, and acceptable for the population. "At the beginning of an insurrection", he wrote, "the insurgent starts out with nothing but a cause and grows to strength,

while the counterinsurgent often starts with everything but a cause and gradually declines in strength to the point of weakness". The cause is instrumental because *it is not only a goal, but also an asset* to ensure support and supply, recruitment and legitimacy.

Furthermore, as Galula emphasized, an insurgency is a competition of two causes. Nevertheless, he failed to describe how causes compete. Indeed, having a better political project and an alternative sustainable ideology is not sufficient to promote it to the target population. It is necessary that the population know it, believe in in and finally be able to defend it. Thus, many French psychological operations in Algeria aimed at questioning the viability of the FLN project while promoting political reforms and the advantages of French citizenship.

As long as the balance of forces is strongly unfair, the fight mostly takes place in the area of ideas. Indeed, the insurgents do not have enough strength actually to threaten the state's existence. Conversely, the lack of concentrated forces denies the counter-insurgent substantial assets to destroy and the states hosting an insurgency cannot hold the population tightly enough to capture the key elements of an insurgency. Therefore, the use of violence from both sides does not aim at eradicating physically the enemy but at encouraging the neutral population to choose a side to support.

Consequently, the struggle between ideologies does not take place in a rational debate, but rather in a multi-channelled communication – that is to say, not only traditional (written and verbal) communication, but also non-verbal communication, a set of converging actions that intend on concurring to promote the political project.

Finally, it is increasingly irrelevant to consider an insurgency as an isolated phenomenon. Several variables directly connect the success to international actors. The bordering countries

21

and especially the regional powers usually have interest in the outcomes of an insurgency. Thus, Chinese interests were of tremendous importance in the conduct of the Vietnam War. Similarly, a solution in Afghanistan has to take into account Pakistani and Iranian interests, because these two countries have the ability to influence the politics in the region in the long term – which an external coalition cannot do, and a political solution that would not be acceptable to them has therefore little (if any) chance to succeed.

Military information operations constitute a comprehensive way of operating in the infosphere, but they are always meant as a support to the "real stuff", the operations on the ground aiming at eradicating the insurgency. On the contrary, an effective strategy should consider the *battle of ideas* as the real goal of a counterinsurgency campaign, and the use of military and civil forces should be considered for their communication outcomes. As Vinciguerra stated, "The IOs should not be considered independently from the global maneuver, but as a full part of it, and to some extent as the dorsal spine of it[27]".

Informational strategies toward populations at stake

Mao Zedong promoted an original way to fight the first stage of an insurgency[28]. For him, the Popular Army had to be accompanied by a political branch that would indoctrinate the populations, so that even if the village happens to be taken by the counterinsurgents, the support of the indoctrinated populations would remain. Similarly, the whole approach Galula advocated in Counterinsurgency Manual aims at gaining the support of local populations.

Information warfare against insurgents

An informational approach is also very useful to dismantle an insurgency. Besides cutting its support and drying up its supplies, an informational strategy aimed at the insurrectional group can also cause it to lose its momentum and fall apart.

One of the purposes of Psyops is precisely to disrupt the enemy's internal coherence. Thus, the British counterinsurgency campaign in Malaya included several actions directed towards the insurgents. For instance, aircraft broadcast mothers' call for their sons to leave the insurgency and come back to the village. Another significant success, they dropped or distributed leaflets that showed themselves to be so effective that an insurgent possessing such leaflets was threatened of death by his peers. [29]

As far as global insurgencies are concerned, Kilkullen advocated: "A strategy of disaggregation would seek to dismantle, or break up, the links that allow the *jihad* to function as a global entity."[30] To understand this strategy, it is important to grasp the nature of this phenomenon. Global *jihad* takes advantage of several local grievances and presents the holy *jihad* as a way to solve these problems. The uniqueness of this movement is that these separate movements have very little cultural commonalities to share, according to Rick and Hecker[31] and yet they managed to federate and created a set of artificial links into a comprehensive movement. The internet, helped build and broadcast a shared ideology, but also allowed promoting a narrative creating a feeling of shared history and destiny. They also developed personal links, fighting together in Afghanistan, and reinforced these through marriages. So, this strategy of disaggregation aims at destroying the links of a *cohesive* nature. Therefore, information operations are the core of this strategy. Indeed, "The center of gravity of Al-Qaeda and other terrorist groups lies in the information domain *"[32]*.

Finally, information operations can "directly attack the enemy's symbols to transform the perceived reality."[33] Thus, according to the USAF Doctrine on Information Operations, "Military deception misleads or manages the perception of adversaries, causing them to act in accordance with friendly objectives."[34] Therefore, this indirect use of information directly attacks the operational effectiveness of the enemy.

Information and international support

Finally, the international support is of critical importance for both sides of an insurrection. Thus, for instance, the Algerian National Liberation Front - the FLN organized a series of strikes beginning in January 28, 1957. According to Horne, "the principle of the strike followed as a direct consequence of the priority of externalizing the country (…). It was to coincide with the opening of the UN session."[35] Thus, the communication of the FLN explained that this event was

"(...) to demonstrate in the most decisive manner the total support of the whole Algerian people for the FLN, its unique representative. The object of this demonstration is to bestow an incontestable authority upon our delegates at the UN in order to convince those rare diplomats still hesitant or possessing illusions about France's liberal policy."[36]

This popular support not only provided a moral caution to their fight. It also fostered support from countries like Morocco (which provided safe sanctuary and weapons), while undermining French popular support to this war.

5.3.Kinetic actions and communication

Defining a strategy focused on Informational issues does not exclude kinetic actions. In fact, the use of violence is a very effective vector in an informational approach that generates several effects. For instance, Paul and Marie-Catherine Villatoux described the intertwinement of

psychological warfare and kinetic operations as "hunting tactics" used by the French Army in Algeria. "The purpose is then to create a permanent feeling of insecurity within the enemy, and hunt them in the areas considered as pacified."[37]

The use of force in a psychological warfare can take several forms. The threat of violence (much more than violence itself, Jenkins argued) is the basic for deterrence. Thus, the French Air Force has increasingly employed the "show of force" as a way to disperse insurgents in Afghanistan, a method deemed more effective and offering less risks of collateral drawbacks than ground attack[38]. Moreover, a local stake between insurgents and counterinsurgents is the security of the neutral population. A measured use of force can therefore provide security to the population and insecurity to the insurgents (as long as the counterinsurgent is able to discriminate the insurgent from the population).

The results of such activities are visible and tangible, thus much more effective than broadcasting messages (although they are more effective when accompanied by adequate communication).

Nevertheless, the use of violence must be carefully balanced. Indeed, violence has different meanings and levels of acceptability according to culture. Due to the global range of information, events that could be locally considered an acceptable level of violence following the situation would look barbarian in other places and create undesired outcomes.

5.4. Control of the infosphere

In the informational sphere, the insurgents, states, are actors as well as public media (newspapers, journalists, etc.), and the minds of the targeted population. The notion of control of this dimension has to be refined. Lonsdale wrote, "Echoing Sir Julian Corbett's theory on sea

power, at the global level the infosphere will commonly remain in an uncommanded state."[39] Thus he proposes the following definition: "Control of the infosphere can be defined as the ability to use the infosphere for the furtherance of strategic objectives while denying the enemy from doing the same."[40] Although this perspective would be extremely favorable, some actors just cannot be controlled. Indeed, the independence of the public media is sacred in many democratic countries, and those which are not independent quickly lose a lot of their credibility, and therefore the effectiveness of the messages. Besides, as long as the insurgency is effective, it has some kind of control over its own troops and the neutral populations located in their area of influence.

Therefore, it is much more interesting to deal with a *local control of the infosphere*. This local control, for a given group of individual, defines the ability to manipulate the infosphere to transmit messages *effectively* to the target population with a *good rate of acceptance* while denying this capability to the enemy. This definition differs in several ways:

- It is narrower in range, because if one considers the international support, or the homeland (in the case of a foreign or transnational insurgency), control of the infosphere is not attainable and the concept is therefore of no use;

- It is broader in meaning, because it does not only encompass the technical ways to bring a message to the populations, it also examines the likeliness that this message be understood and accepted.

Achievement of local control must also take into account the interactions between infospheres. Indeed, as we already argued, information flows from an infosphere to another, from a local area to the international stage.

Several typical strategies can help achieve control of an infosphere.

5.5. Strategy of interdiction

A strategy of interdiction describes an action preventing the insurgent (or the counterinsurgent) from accessing the key population, interdicting thus any influence. This strategy was widely used by insurgents in remote areas, where the counterinsurgent could not maintain a continuous presence, and where the direct contact remained the most effective communication.

Thus Mao's strategy, first used in China, then replicated in Indochina and to a lesser extent in South Vietnam, aimed at gradually expelling all state influence at the local level (villages), in order to impose the insurgent's political model. This strategy is followed as well by counter-insurgent. Indeed, when the communications were primitive, and when the villages could be isolated, the "new villages" in Malaya or the protected villages in Indochina allowed the counterinsurgents to impose their messages, forbid any access of the insurgents (deprive the "fish" from its natural element). In today's interconnected world, this strategy must encompass the new dimensions offered by public media and data communications.

5.6. Strategy of disaggregation

In contrast, a strategy of disaggregation does not aim at prevailing in a given Infosphere. Instead, it aims at penetrating an infosphere in order to destroy the cohesive links of the enemy. This strategy has been the base of psychological warfare.

This approach tends to undermine the enemy's cohesion and outmaneuver him so that his size does no longer allow him to adapt and forces it to break down into smaller cells.

6. Conclusion

While most conflicts of the post-World War 2 era have included an insurrectional-type component, this kind of phenomenon remains widely misunderstood today. Indeed, its complexity made of the intertwinement of political, ideological, economic and societal issues now becomes even harder to grasp with the advent of transnational movements that add an international layer to this maelstrom.

Several approaches have tried to offer a unifying model to grasp the issues of an insurgency and design an effective strategy. The enemy-centric approach reflects the tendency of conventional armies to find and destroy the enemy. Effective when the insurgency is not able to hide within the population, it does not address any of the roots of an insurrection. Moreover, disregarding the population, it deprives the counterinsurgent of popular assistance and helps the insurgency recruit more soldiers.

The population-centric approach, first implemented by Gallieni and popularized by Lyautey and Galula, took this concern into account. Therefore, it advocated a strategy aiming at providing security to the population inside a restricted perimeter, interdicting the insurgents within this area, so that the population would support the counterinsurgency campaign, provide intelligence and in some cases eventually ensure its own security.

Finally, some recent approaches emphasize the critical role of leadership in fighting insurgencies. Thus Moyar advocated the importance of adaptive and creative leaders, while Nagl linked the success of counterinsurgents to the ability of the organization to learn and quickly adapt to the insurgency's tactics, in order to outmaneuver it.

Nevertheless, none of these approaches have fully succeeded in explaining all the components of the phenomenon. Thus, enemy-centric strategies simply fail to understand the operational environment. Indeed, the insurgency takes its strengths and haven in the population at stake. Population-centric approaches grasp some essential tenets of an insurgency, but fail to explain how the competition of two causes materializes in the eyes of the international community and the populations at stake. Finally, leadership-centric approaches are more enablers of a strategy and do not help understanding the phenomenon.

Besides, recent developments of irregular warfare make the task of grasping insurgencies even more complex. Indeed, several technological and societal evolutions have dramatically modified the face of war. As a consequence, Information has become an ecosystem of critical importance, has challenged the supremacy of States and has granted new operational and strategic opportunities to the insurgents.

Therefore it is important to examine the tenets of the Infospheres. They are informational ecosystems, including individual actors consuming and generating information, but also technical and social systems that convey (and sometimes modify) this information. Armies and counterinsurgents have adapted to this new environment in very different ways. While the technological leap provided the insurgents with unprecedented ways to command and control, structure, recruit and wage a communication war, the regular armies were hampered by the division between the military and political levels of communication.

Given all these variables, it is consequently possible to state that modern insurgencies are best described as an informational competition where communication is key. Indeed, due to the very nature of an insurgency, the competition of ideologies takes place in the perceptions of the

populations at stake. Moreover, the publicity of today's conflicts makes the outcomes of communication instrumental in providing support, maintaining one's "will to fight" while degrading it among one's enemies. To do so, several complementary strategies can pursue this goal. A strategy of interdiction aims at gaining access to an Infosphere while preventing the enemy from having any influence in it. Besides, a strategy of disaggregation will destroy the links that keep the enemy together. While a traditional enemy-centric approach attacks the functional links of the enemy to neutralize him, this strategy threatens the cohesive, internal links that unite the insurgents.

The History of insurrectional warfare has showed that insurgents have sought to expand their fight to new areas in order to challenge an enemy that would not be attackable otherwise. As a consequence, the counterinsurgents face a paradox: fight according to their own rules and risk being defeated, or expand the military powers and responsibilities to address successfully the paradigms imposed by their enemy. It is astonishing to notice that the most successful campaigns were won by leaders who had been granted some kind of administrative and political powers (Gallieni in Indochina, Templer in Malaya). Is it to say that the multifaceted nature of insurrections (economic, societal, military, political) advocates for a shift in the civil-military share of responsibilities?

Notes

---

[1] Von Clausewitz, Carl. *"On War",* p91

[2] Callwell, C.E., Small Wars: Their Principles and Practices

[3] Galula, David. "Counterinsurgency Warfare, Theory and Practice", p4.

[4] Galula, David. "Counterinsurgency Warfare, Theory and Practice", p4

[5] Moyar , Mark. A Question of Command. p3

[6] Merom, Gil, *How Democracies lose Small* Wars, Cambridge University Press, p34

[7] Jenkins, Clinton. *The psychological nature of Risk.*

[8] Kilkullen, David. *Countering Global Insurgency*, p15-18

[9] Lonsdale, David J. The nature of War in the Information Age, p181

[10] Floridi, Luciano. *A look into the future impact of ICT on our lives*. P3

[11] Hoskins Andrew. *Televising wars, from Vietnam to Iraq.*

[12] Rid, Thomas and Hecker, Mark. War 2.0: *: Irregular Warfare in the Information Age*

[13] Rid, Thomas and Hecker, Mark. War 2.0: *: Irregular Warfare in the Information Age*, loc.119 (Kindle)

[14] Rid, Thomas and Hecker, Mark. War 2.0: *: Irregular Warfare in the Information Age*, loc958(Kindle)

[15] Rid, Thomas and Hecker, Mark. War 2.0: *: Irregular Warfare in the Information Age*, loc221(Kindle)

[16] Cloud, David and Jaffe, Greg. *The Fourth Star*, p236

[17] AFDD3-13. *Information Operations*, p15.

[18] French Joint Headquarters. *DIA 3-10, Joint Doctrine on Information Operations*, p9

[19] Rid, Thomas and Hecker, Mark. *War 2.0: : Irregular Warfare in the Information Age*, loc108(Kindle)

[20] Rid, Thomas and Hecker, Mark. *War 2.0: : Irregular Warfare in the Information Age*, loc556(Kindle)

[21] Rid, Thomas and Hecker, Mark. *War 2.0: : Irregular Warfare in the Information Age*

[22] Galula, David. *"Counterinsurgency Warfare, Theory and Practice"*,

[23] Galula, David. *"Counterinsurgency Warfare, Theory and Practice*, p75

[24] Nagl, John. *Learning to Eat Soup with a Knife*, p93

[25] Sharlet, http://harpers.org/archive/2009/05/0082488

[26] Von Clausewitz, Karl. *On War.*

[27] Vinciguerra, Isabelle. "*Les operations d'information: mythe ou réalité?",* in Cahiers du CESA, p116

[28] Mao Zedong. "Strategy in China's Revolutionary War." In Gerard Chaliand. The Art of War in World History: From Antiquity to the Nuclear Age. Berkeley: University of California Press, 1994. Pp. 976-990.

[29] Jackson, XXXX. *The Malayan Emergencies.*

[30] Kilkullen, David. *Countering Global Insurgency*. P37

[31] Rid, Thomas and Hecker, Mark. War 2.0: *: Irregular Warfare in the Information Age*

[32] Rid, Thomas and Hecker, Mark. War 2.0: *: Irregular Warfare in the Information Age*, loc961(Kindle)

[33] Rouquet, Michel. *Point sur les operations psychologiques*, p1

[34] AFDD3-13. *Information Operations*, p11

[35] Horne, Alastair. *A savage War of Peace*, p190

[36] Horne, Alastair. *A savage War of Peace*, p190

[37] Villatoux, Paul and Marie-Catherine. "*La Republique et son Armée face au Péril Subversif*"(The Republic and its Army against the subversive threat), p516

[38] Vinciguerra, Isabelle. "*Les operations d'information: mythe ou realité?",* in Cahiers du CESA, p115

[39] Lonsdale, David J. The nature of War in the Information Age, p185

[40] Ibid. p185

Bibliography

Callwell, C.E., *Small Wars: Their Principles and Practices*, University of Nebraska Press, 1996

Clausewitz, Carl. *On War.* Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. Praeger Publishers, 2006.

Lonsdale, David. *The nature of War in the Information Age*. Frank Cass, 2004.

Mao Zedong. "*Strategy in China's Revolutionary War*." In Gerard Chaliand. *The Art of War in World History: From Antiquity to the Nuclear Age*. Berkeley: University of California Press, 1994.

Merom, Gil, *How Democracies lose Small* Wars, Cambridge University Press, 2003.

Moyar Mark. *A Question of Command: Counterinsurgency from the Civil War to Iraq*. New Haven: Yale University Press, 2009.

Nagl, John A.. *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*. Chicago: University of Chicago, 2002.

AFDD3-13. *Information Operations*

French Joint Headquarters. *DIA 3-10, Joint Doctrine on Information Operations*

Jenkins, Clinton. *The psychological nature of Risk*

Kilkullen, David. *Countering Global Insurgency*. In Small Wars Journal, 2004

Floridi, Luciano. *A look into the future impact of ICT on our lives*.

Hoskins Andrew. *Televising wars, from Vietnam to Iraq*. Continuum, 2004

Rid, Thomas and Hecker, Mark. War 2.0: *: Irregular Warfare in the Information Age*, Praeger, 2009(Kindle Edition)

Cloud, David and Jaffe, Greg. *The Fourth Star*, Three Rivers Press, 2010

Sharlet, Jeff. *Jesus killed Mohammed:The crusade for a Christian military*. In Harper's Magazine, May 2009. (http://harpers.org/archive/2009/05/0082488)

Vinciguerra, Isabelle. "*Les operations d'information: mythe ou realité?",* in « Penser les Ailes Francaises », nr 17

Jackson, Robert. *The Malayan Emergency and Indonesian Confrontation*. Pen & Sword, 2008

Rouquet, Michel. *Point sur les operations psychologiques*, AEGE, 2009 (http://bdc.aege.fr/public/Point_sur_les_operations_psychologiques.pdf)

Horne, Alastair. *A savage War of Peace*. New York Review of Books, 2006

Villatoux, Paul and Marie-Catherine. "*La Republique et son Armée face au Péril Subversif*"(The Republic and its Army against the subversive threat), Les Indes Savantes, 2005